Twisted Reed-Solomon Codes

Beelen, Peter ; Puchinger, Sven; Rosenkilde ne Nielsen, Johan

Published in:
Proceedings of 2017 IEEE International Symposium on Information Theory

Link to article, DOI:
10.1109/ISIT.2017.8006545

Publication date:
2017

Document Version
Peer reviewed version

Twisted Reed–Solomon Codes

Peter Beelen[1], Sven Puchinger[2], and Johan Rosenkilde né Nielsen[1]

[1]Department of Applied Mathematics & Computer Science, Technical University of Denmark, Lyngby, Denmark
[2]Institute of Communications Engineering, Ulm University, Ulm, Germany
Email: *pabe@dtu.dk, sven.puchinger@uni-ulm.de, jsrn@jsrn.dk*

***Abstract*—We present a new general construction of MDS codes over a finite field $\mathbb{F}_q$. We describe two explicit subclasses which contain new MDS codes of length at least $q/2$ for all values of $q \geq 11$. Moreover, we show that most of the new codes are not equivalent to a Reed–Solomon code.**

***Index Terms*—MDS Codes, Reed–Solomon Codes**

I. Introduction

A *maximum distance separable* (MDS) code $\mathcal{C}(n, k, d)$ of length n, dimension k, and minimum distance d is a linear code attaining the Singleton bound, i.e., $d = n - k + 1$ [1]. The most prominent MDS codes are *generalized Reed–Solomon* (GRS) codes [2]. However, there are many other known constructions for MDS codes, e.g., based on the equivalent problem of finding n-arcs in projective geometry [3], circulant matrices [4], Hankel matrices [5], or extending GRS codes.

Recently, Sheekey [6] introduced a new class of *maximum rank distance* codes—which are MDS in terms of the *rank metric*. These codes, *Twisted Gabidulin* codes, were shown to be not equivalent to Gabidulin codes (the rank-metric analogues of Reed–Solomon codes).

In this paper, we introduce a new construction of Hamming-metric MDS codes, inspired by [6]. The idea is to evaluate polynomials of the form

$$f(x) = a_0 + a_1 x + \ldots + a_{k-1}x^{k-1} + \eta a_h x^{k-1+t},$$

for some $0 \leq h < k$ and $t < n - k$. By a prudent choice of t, h and η, we ensure that any such polynomial has at most $k - 1$ zeroes among the evaluation points, even though their degree is larger than $k - 1$. This is enough to ensure that the resulting code is MDS.

We single out two explicit subclasses of this construction where the MDS property can be a priori ensured. These contain codes of length up to roughly $q/2$ for any q, and we show that for $q \geq 11$, they contain non-GRS MDS codes.

The results we obtain are somewhat reminiscent of results in [4], where non-GRS MDS codes were constructed of length roughly $q/2$ for even q. However, our construction is very different, and for small values of q we verified using a computer that our construction produces codes inequivalent to the ones mentioned in [4]. More importantly, our construction also gives a very simple way to produce non-GRS MDS codes of length at least $q/2$ if q is odd and $q \geq 11$.

Besides adding new codes to the family of known MDS codes, the new code class might be interesting for code-based cryptography. As future work, we will analyze whether our codes or their subfield subcodes are suitable for this purpose.

II. Preliminaries

In this section, we recall several definitions and known results for future use in the paper. We denote by $\mathbb{F}_q$ the finite field with q elements.

Definition 1 ([7]): Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q \cup \{\infty\}$ be distinct, $k < n$, and $v_1, \ldots, v_n \in \mathbb{F}_q^*$. The corresponding *generalized Reed–Solomon (GRS) code* is defined by

$$\mathcal{C}_{n,k}^{\mathrm{GRS}} = \{[v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)] : f \in \mathbb{F}_q[x], \deg f < k\}.$$

In this setting, for a polynomial f of degree $\deg f < k$, the quantity $f(\infty)$ is defined as a_{k-1}, the coefficient of x^{k-1} in the polynomial f.

In case $v_i = 1$ for all i, the code is called a *Reed–Solomon (RS) code*. Any non-zero evaluation polynomial f is of degree $\deg f < k$ and hence has at most $k - 1$ roots among the evaluation points $\alpha_1, \ldots, \alpha_n$ in $\mathbb{F}_q$. If $f(\infty)$ "evaluates" to zero, this just means that $\deg f < k - 1$ and hence f has at most $k - 2$ roots among the remaining evaluation points. This proves that a GRS code is MDS.

In this article, we will construct MDS codes of length n and dimension k using spaces of polynomials that may contain elements of degree $\deg f \geq k$. To define our codes, we will use the following map.

Definition 2: Let $\mathcal{V} \subset \mathbb{F}_q[X]$ be a k-dimensional $\mathbb{F}_q$-linear subspace. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q \cup \{\infty\}$ be distinct and write $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_n]$. We call $\alpha_1, \ldots, \alpha_n$ the *evaluation points*. Then we define the *evaluation map* of $\boldsymbol{\alpha}$ on $\mathcal{V}$ by

$$\mathrm{ev}_{\boldsymbol{\alpha}}(\cdot) : \mathcal{V} \to \mathbb{F}_q^n, \quad f \mapsto [f(\alpha_1), \ldots, f(\alpha_n)].$$

Here $f(\infty)$ is defined as a_ℓ, the coefficient of x^ℓ in the polynomial $f \in \mathcal{V}$, where $\ell := \max \deg\{f : f \in \mathcal{V}\}$.

The evaluation map above is $\mathbb{F}_q$-linear. This means in particular that if for a given $\mathcal{V}$ the evaluation map is injective, then the code $\mathrm{ev}_{\boldsymbol{\alpha}}(\mathcal{V}) \subset \mathbb{F}_q^n$ will be an $\mathbb{F}_q$-linear code of length n and dimension k. Injectivity is immediate if $\ell < n$. If $\mathcal{V}$ consists of all polynomials of degree strictly less than k, the resulting code is an RS code. For other choices of $\mathcal{V}$, the resulting code might still be *equivalent* to an RS code; we use the following notion of code equivalence.

Definition 3: Let $\mathcal{C}_1, \mathcal{C}_2$ be $\mathbb{F}_q$-linear $[n, k]$ codes. We say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are *equivalent* if there is a permutation $\pi \in S_n$ and $\boldsymbol{v} := [v_1, \ldots, v_n] \in \left(\mathbb{F}_q^*\right)^n$ such that $\mathcal{C}_2 = \varphi_{\pi,\boldsymbol{v}}(\mathcal{C}_1)$ where $\varphi_{\pi,\boldsymbol{v}}$ is the Hamming-metric isometry

$$\varphi_{\pi,\boldsymbol{v}} : \mathbb{F}_q^n \to \mathbb{F}_q^n, \quad [c_1, \ldots, c_n] \mapsto [v_1 c_{\pi(1)}, \ldots, v_n c_{\pi(n)}].$$

It is clear from the above definition that a code is a GRS code if and only if it is equivalent to an RS code. The following well-known theorem provides an effective tool to decide whether a code is equivalent to an RS code.

Theorem 1 ([5], [8]): A linear code with generator matrix $\boldsymbol{G} = [\boldsymbol{I} \mid \boldsymbol{A}]$ is a GRS code if and only if

(i) All entries of $\boldsymbol{A}$ are non-zero.
(ii) All 2×2 minors of $\tilde{\boldsymbol{A}}$ are non-zero, and

(iii) All 3×3 minors of $\tilde{\boldsymbol{A}}$ are zero,

where $\tilde{\boldsymbol{A}} \in \mathbb{F}_q^{k \times n-k}$ is given by $\tilde{A}_{ij} = A_{ij}^{-1}$.

Note that any MDS code has a generator matrix of the form $\boldsymbol{G} = [\boldsymbol{I} \mid \boldsymbol{A}]$ and that items (i) and (ii) above are satisfied for this A. Hence the difference between GRS and non-GRS MDS codes will only become apparent using item (iii). If $k < 3$ or $n - k < 3$, the matrix A has no 3×3 minors, so the following corollary holds.

Corollary 2: Suppose that $k < 3$ or $n - k < 3$. Any MDS code of length n and dimension k is equivalent to an RS code.

We finish this section by quoting results on t-sum generators in abelian groups from [4], [9]. We will apply these results to the abelian groups $(\mathbb{F}_q^*, \cdot)$ and $(\mathbb{F}_q, +)$ to analyse several instances of our code construction in the coming sections.

Definition 4 ([9]): Let $(A, \oplus)$ be a finite abelian group and $k \in \mathbb{N}$. A subset $S \subset A$ is called a *k-sum generator* of A if for all $a \in A$, there are distinct $s_1, \ldots, s_k \in S$ such that $a = \bigoplus_{i=1}^{k} s_i$. We denote by $M(k, A)$ the smallest integer such that any $S \subset A$ with $|S| > M(k, A)$ is a k-sum generator of A.

Lemma 3 ([9, Theorem 3.1]): Let $|A| = 2r$ for some $r \geq 6$. Then, for any $3 \leq k \leq r - 2$,

$$M(k, A) = r,$$

except if $A \in \{\mathbb{Z}_2^m, \mathbb{Z}_4 \times \mathbb{Z}_2^{m-1}\}$ for some $m > 1$ and $k \in \{3, r - 2\}$ in which case

$$M(k, A) = r + 1.$$

This lemma suffices for our purposes. See [4], [9] for more information in case $|A|$ is odd.

III. Twisted Reed–Solomon Codes

In this section, we present our new code construction. Similar to RS codes, we evaluate polynomials whose first k coefficients we can choose arbitrarily. The difference is that we allow another monomial of degree larger than $k-1$ to occur in the polynomials as well. We define a set of evaluation polynomials as follows.

Definition 5: Let $k, t, h \in \mathbb{N}$ such that $0 \leq h < k \leq q$ and let $\eta \in \mathbb{F}_q \backslash \{0\}$. Then, we define the set of *(k, t, h, η)-twisted polynomials* by

$$\mathcal{V}_{k,t,h,\eta} = \left\{ f = \sum_{i=0}^{k-1} a_i x^i + \eta a_h x^{k-1+t} : a_i \in \mathbb{F}_q \right\},$$

where we call h the *hook* and t the *twist*.

Note that $\mathcal{V}_{k,t,h,\eta} \subseteq \mathbb{F}_q^n$ is a k-dimensional $\mathbb{F}_q$-linear subspace. Using the evaluation map from Definition 2 for $\mathcal{V} = \mathcal{V}_{k,t,h,\eta}$, we obtain the codes that we will study in this article.

Definition 6: Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q \cup \{\infty\}$ be distinct and write $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_n]$. Let k, t, h, η be chosen as in Definition 5 such that $k < n$ and $t \leq n - k$. Then, the corresponding *twisted Reed–Solomon code* of length n and dimension k is given by

$$\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta) = \mathrm{ev}_{\boldsymbol{\alpha}}(\mathcal{V}_{k,t,h,\eta}) \subseteq \mathbb{F}_q^n.$$

For brevity, we will use the phrase *twisted codes* rather than *twisted Reed–Solomon codes* from now on. Note that $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ indeed has dimension k since the evaluation map is injective: any polynomial $f \in \mathcal{V}_{k,t,h,\eta}$ satisfies $\deg f \leq k - 1 + t < n$. In principle η could be 0 in the above definition, but in that case we simply obtain RS codes.

IV. MDS Twisted Codes

In general, twisted codes are not MDS for all parameters $\boldsymbol{\alpha}, k, t, h, \eta$. However, in this section we will describe several classes of twisted codes that are always MDS.

A. $(*)$-twisted Codes

If $(t, h) = (1, 0)$, it is possible to give a succinct condition on when the code $\mathcal{C}_k(1, 0, \eta, \boldsymbol{\alpha})$ is MDS. More precisely, we have the following:

Lemma 4: Let $k < n$, $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ distinct and $\eta \in \mathbb{F}_q$. Then the twisted code $\mathcal{C}_k(\boldsymbol{\alpha}, 1, 0, \eta)$ is MDS if and only if

$$\eta(-1)^k \prod_{i \in \mathcal{I}} \alpha_i \neq 1 \quad \forall \mathcal{I} \subseteq \{1, \ldots, n\} \text{ s.t. } |\mathcal{I}| = k. \tag{1}$$

Proof: The code is MDS if and only if the only polynomial of the required form which has k roots among the α_i is the zero polynomial. Let $f = \sum_{i=0}^{k-1} a_i x^i + \eta a_0 x^k$ be such a polynomial. In the first place $a_0 \neq 0$, since otherwise $\deg f < k$, making it impossible that f has k roots among the α_i. If there is a subset $\mathcal{I} \subseteq \{1, \ldots, n\}$ with $|\mathcal{I}| = k$ and $f(\alpha_i) = 0$ for all $i \in \mathcal{I}$, we can write $f = \eta a_0 \prod_{i \in \mathcal{I}} (x - \alpha_i)$ and considering the constant term it follows that

$$1 = \eta(-1)^k \prod_{i \in \mathcal{I}} \alpha_i. \tag{2}$$

If Condition (1) is satisfied, no such f can exist. Conversely, if there is an $\mathcal{I}$ such that $\eta(-1)^k \prod_{i \in \mathcal{I}} \alpha_i = 1$, then $\eta \neq 0$ and $f = \eta \prod_{i \in \mathcal{I}} (x - \alpha_i) \in \mathcal{V}_{k,t,h,\eta}$ has k roots among the α_i, so the code is not MDS. ∎

This leads to our first explicit subclass of twisted codes which are MDS[1]:

Definition 7: $\mathcal{C}_k(\boldsymbol{\alpha}, 1, 0, \eta)$ is a *$(*)$-twisted code* if the elements of $\boldsymbol{\alpha}$ are a subset of $G \cup \{0\}$, for G a proper subgroup of $(\mathbb{F}_q^*, \cdot)$, and if $(-1)^k \eta^{-1} \in \mathbb{F}_q^* \setminus G$. We write $\mathcal{C}_k^*(\boldsymbol{\alpha}, \eta) := \mathcal{C}_k(\boldsymbol{\alpha}, 1, 0, \eta)$.

Theorem 5: Any $(*)$-twisted code is an MDS code.

Proof: If a $(*)$-twisted code $\mathcal{C}_k^*(\boldsymbol{\alpha}, \eta)$ is not MDS, then Lemma 4 implies that there exists $\mathcal{I} \subseteq \{1, \ldots, n\}$ such that $(-1)^k \eta \prod_{i \in \mathcal{I}} \alpha_i = 1$. Since the α_i are contained in a subgroup G of $\mathbb{F}_q^*$, we have $\prod_{i \in \mathcal{I}} \alpha_i \in G$, implying that $(-1)^k \eta \in G$ as well. This gives a contradiction. ∎

Corollary 6: Let $\mathbb{F}_q$ be a finite field and let p be a prime divisor of $q - 1$. Then there exists a $(*)$-twisted code of length

$$n = \tfrac{q-1}{p} + 1.$$

In particular, if q is odd, $(*)$-twisted codes can have length $n = \frac{q+1}{2}$.

Proof: The maximum cardinality of a proper subgroup G of $\mathbb{F}_q^*$ is $(q - 1)/p$. Now let $\boldsymbol{\alpha}$ be $G \cup \{0\}$ in some order in Definition 7. ∎

For odd q $(*)$-twisted codes can therefore be rather long. But the choice of $\boldsymbol{\alpha}$ is very limited in Definition 7, and perhaps longer codes could be constructed with $(t, h) = (1, 0)$. The following answers this negatively, by using k-sum generators.

Lemma 7: Let $\eta \in \mathbb{F}_q^*$ and let $S := \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^*$ be a k-sum generator of $(\mathbb{F}_q^*, \cdot)$. Then the twisted code $\mathcal{C}_k(\boldsymbol{\alpha}, 1, 0, \eta)$ is not MDS.

[1]This class can be seen as the Hamming-metric analog of Twisted Gabidulin codes [6]. However, we use different techniques for analyzing our codes.

Proof: By the definition of a k-sum generator, there is an index set $\mathcal{I} \subseteq \{1,\dots,n\}$ with $|\mathcal{I}| = k$ such that $\prod_{i\in\mathcal{I}} \alpha_i = (-1)^k \eta^{-1}$. Hence $\mathcal{C}_k(\boldsymbol{\alpha}, 1, 0, \eta)$ is not MDS by Lemma 4. ∎

Theorem 8: Let $\mathbb{F}_q$ be a finite field, with q odd. Further let $\eta \in \mathbb{F}_q^*$. Then, for any $3 \le k \le \frac{q-1}{2} - 2$, the length n of a twisted code $\mathcal{C}_k(\boldsymbol{\alpha}, 1, 0, \eta)$ which is MDS, satisfies $n \le \frac{q+1}{2}$.

Proof: We know that $(\mathbb{F}_q^*, \cdot)$ is a cyclic abelian group of order $|\mathbb{F}_q^*| = q-1$, which is even since q is a power of an odd prime. Hence Lemma 3 implies

$$M(k, \mathbb{F}_q^*) = \tfrac{q-1}{2}.$$

Now suppose $n > \frac{q+1}{2}$ and $\boldsymbol{\alpha} = [\alpha_1, \dots, \alpha_n]$. Then, $S := \{\alpha_1, \dots, \alpha_n\} \cap \mathbb{F}_q^*$ has cardinality

$$|S| \ge n - 1 > \tfrac{q+1}{2} - 1 = \tfrac{q-1}{2} = M(k, \mathbb{F}_q^*)$$

and is therefore a k-sum generator of $\mathbb{F}_q^*$. By Lemma 7, the code $\mathcal{C}_k(\boldsymbol{\alpha}, 1, 0, \eta)$ is not MDS for any $\eta \neq 0$. ∎

Remark 9: For even $q > 4$, the $(*)$-twisted codes cannot attain length $\lfloor (q+1)/2 \rfloor$. However, we determined by computer search that for e.g. $q = 16$, there are many $[9, k]$ twisted codes with $(t, h) = (1, 0)$ for other choices of $\boldsymbol{\alpha}$ and η, for $k = 3, 4, 5$. See also Section VI.

B. $(+)$-twisted Codes

While the results in the previous subsection were based on properties of the multiplicative group $(\mathbb{F}_q^*, \cdot)$, it is also possible to use the structure of the additive group $(\mathbb{F}_q, +)$. This structure arises when considering the case $(t, h) = (1, k-1)$. We have the following analogue of Lemma 4.

Lemma 10: Let $k < n \le q$, $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$ distinct and $\eta \in \mathbb{F}_q$. Then the twisted code $\mathcal{C}_k(\boldsymbol{\alpha}, 1, k-1, \eta)$ is MDS if and only if

$$\eta \sum_{i\in\mathcal{I}} \alpha_i \neq -1 \quad \forall \mathcal{I} \subseteq \{1,\dots,n\} \text{ s.t. } |\mathcal{I}| = k. \tag{3}$$

Proof: The code is MDS if and only if the only polynomial

$$f = a_0 + \ldots + a_{k-1}x^{k-1} + \eta a_{k-1} x^k \in \mathcal{V}_{k,1,k-1,\eta}$$

having k roots among the α_i is the zero polynomial. If $f \neq 0$ is such a polynomial, there is a subset $\mathcal{I} \subseteq \{1,\dots,n\}$ with $|\mathcal{I}| = k$ and $f(\alpha_i) = 0$ for all $i \in \mathcal{I}$. Writing $f = \eta a_{k-1} \prod_{i\in\mathcal{I}} (x - \alpha_i)$, with $a_{k-1} \neq 0$, we obtain a contradiction by considering the coefficient of x^{k-1} on both sides, since

$$a_{k-1} = -\eta a_{k-1} \sum_{i\in\mathcal{I}} \alpha_i \iff \eta \sum_{i\in\mathcal{I}} \alpha_i = -1$$

Conversely, if there is an $\mathcal{I}$ such that $\eta \sum_{i\in\mathcal{I}} (-\alpha_i) = 1$, then $f = \eta \prod_{i\in\mathcal{I}} (x - \alpha_i)$ is a polynomial of the appropriate form having k roots among the α_i, so the code is not MDS. ∎

As in the previous subsection, this naturally gives rise to a subclass of twisted codes.

Definition 8: $\mathcal{C}_k(\boldsymbol{\alpha}, 1, 0, \eta)$ is a *$(+)$-twisted code* if the elements of $\boldsymbol{\alpha}$ are a subset of $V \cup \{\infty\}$, for V a proper subgroup of $(\mathbb{F}_q, +)$, and if $\eta^{-1} \in \mathbb{F}_q \backslash V$. We write $\mathcal{C}_k^+(\eta, *) := \mathcal{C}_k(\boldsymbol{\alpha}, 1, 0, \eta)$.

The analysis of these codes follows that of their multiplicative counterparts from the previous subsection very closely. In particular we have the following:

Theorem 11: Any $(+)$-twisted code is an MDS code.

Proof: We simply apply Lemma 10 instead of Lemma 4. Some care must be taken that adding ∞ to a set of evaluation points preserves the MDS property. However, if a polynomial $f \in \mathcal{V}_{k,1,k-1,\eta}$ satisfies $f(\infty) = 0$, that means its degree is at most $k-2$. ∎

Corollary 12: Let $\mathbb{F}_q$ be a finite field of characteristic p. Then there exists a $(+)$-twisted code of length

$$n = \tfrac{q}{p} + 1.$$

In particular, if q is even, $(+)$-twisted codes can have length $n = \frac{q}{2} + 1$.

Proof: The maximum cardinality of a proper subgroup V of $\mathbb{F}_q$ is q/p. Now set $S = \{\infty\} \cup V$ in Definition 8. ∎

Lemma 7 and Theorem 8 have a direct analogue as well. For completeness, we state the results, but since the proofs are extremely similar, we leave these to the reader.

Lemma 13: Let $\eta \neq 0$ and $S := \{\alpha_1, \dots, \alpha_n\} \in \mathbb{F}_q$ be a k-sum generator of $(\mathbb{F}_q, +)$. Then the twisted code $\mathcal{C}_k(\boldsymbol{\alpha}, 1, k-1, \eta)$ is not MDS.

Theorem 14: Let $\mathbb{F}_q$ be a finite field, with q even. Further let $\eta \in \mathbb{F}_q^*$. Then, for any $3 \le k \le \frac{q}{2} - 2$, the length n of a twisted code $\mathcal{C}_k(\boldsymbol{\alpha}, 1, k-1, \eta)$ which is MDS, satisfies $n \le \frac{q}{2} + 1$ if $3 < k < \frac{q}{2} - 3$ and $n \le \frac{q}{2} + 2$ if $k \in \{3, \frac{q}{2} - 2\}$.

C. General Theory of Twisted Codes

For general t and h, it is still possible to derive a criterion for a code $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ to be MDS. We do so in the following lemma, generalizing Lemmas 4 and 10.

Lemma 15: Let $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$ and define for $\mathcal{I} \subseteq \{1,\dots,n\}$ the polynomial $\sum_i \sigma_i x^i := \prod_{i\in\mathcal{I}} (x - \alpha_i)$, where $\sigma_i := 0$ for $i < 0$. The twisted code $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ is MDS if and only if the matrix

$$\underbrace{\begin{bmatrix} \eta^{-1} - \sigma_{h-t+1} & -\sigma_{h-t+2} & \dots & -\sigma_h & & \\ \sigma_{k-1} & 1 & & & & \\ \sigma_{k-2} & \sigma_{k-1} & 1 & & & \\ \sigma_{k-3} & \sigma_{k-2} & \sigma_{k-1} & 1 & & \\ \vdots & \ddots & \ddots & \ddots & \ddots & \\ \sigma_{k-t+1} & \dots & \sigma_{k-3} & \sigma_{k-2} & \sigma_{k-1} & 1 \end{bmatrix}}_{=: \boldsymbol{A}_{\mathcal{I}} \in \mathbb{F}_q^{t\times t}},$$

is regular for all $\mathcal{I} \subseteq \{1,\dots,n\}$ such that $|\mathcal{I}| = k$.

Proof: Let $f \in \mathcal{V}_{k,t,h,\eta}$ be a polynomial with at least k roots among the α_i's. Then, there is an index set $\mathcal{I} \subseteq \{1,\dots,n\}$ with $|\mathcal{I}| = k$ and $f(\alpha_i) = 0$ for all $i \in \mathcal{I}$. We can factor f into $f(x) = g(x) \cdot \sigma(x)$, with

$$g(x) = \sum_{i=0}^{t-1} g_i x^i, \quad \sigma(x) = \sum_{i=0}^{k} \sigma_i x^i := \prod_{i\in\mathcal{I}} (x - \alpha_i).$$

Note that $\sigma_k = 1$. Since by construction, the coefficients in f to $x^k, \dots, x^{k+t-2}$ are zero, we obtain the following system of $(t-1)$ equations in the g_j's,

$$0 = \sum_{j=0}^{i} g_j \sigma_{i-j} \quad i = k, \dots, k+t-2, \tag{4}$$

where $g_j := 0$ for all $j \notin \{0,\dots,t-1\}$, and $\sigma_j := 0$ for $j \notin \{0,\dots,k\}$. Considering the coefficients of x^{k-1+t} and x^h, we obtain $\eta a_h = g_{t-1}$ and $a_h = \sum_{j=0}^{h} g_j \sigma_{h-j}$ and hence

$$0 = \eta^{-1} g_{t-1} - \sum_{j=0}^{h} g_j \sigma_{h-j}. \tag{5}$$

Equations (4) and (5) result in a homogeneous system of t equations in t variables $\boldsymbol{g} := [g_{t-1}, g_{t-2}, \ldots, g_0]^{\mathrm{T}}$:

$$\boldsymbol{A}_{\mathcal{I}} \cdot \boldsymbol{g} = \boldsymbol{0} \tag{6}$$

The code $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ is MDS if and only if the only polynomial $f \in \mathcal{V}_{k,t,h,\eta}$ with at least k roots is the zero polynomial, which holds if and only if the system (6) has only the zero vector as solution for all choices of index sets $\mathcal{I} \subseteq \{1, \ldots, n\}$ with $|\mathcal{I}| = k$. This implies the claim. ∎

Remark 16: If one includes ∞ as evaluation point and $h = k - 1$, the above lemma is still true when considering $\mathcal{I}$ not containing ∞. Indeed if $f(\infty) = 0$, then $\deg f < k - 1$, which means the MDS property is not affected.

As we will see in Section VI many long MDS codes can be obtained using twisted codes for particular values of q. Hence an upper bound like in Theorems 8 and 14 does not hold for general h and t. On the other hand, it seems harder to find explicit constructions of such long MDS codes. We do have the following result.

Theorem 17: Let $\mathbb{F}_s \subsetneq \mathbb{F}_q$ be a proper subfield and $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_s$. If $\eta \in \mathbb{F}_q \setminus \mathbb{F}_s$, then the twisted code $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ is MDS.

Proof: Let $\eta \in \mathbb{F}_q \setminus \mathbb{F}_s$. Let $\mathcal{I} \subseteq \{1, \ldots, n\}$ be an index set with $|\mathcal{I}| = k$ and $\boldsymbol{A}_{\mathcal{I}}$ be the corresponding matrix as in Lemma 15. Using elementary row operations, we can bring $\boldsymbol{A}_{\mathcal{I}}$ into lower triangular form with diagonal elements $\eta^{-1} + T, 1, \ldots, 1$ for a certain $T \in \mathbb{F}_q$. Using that $\sigma_i \in \mathbb{F}_s$ for all i (since the same holds for all α_i), we conclude that in fact $T \in \mathbb{F}_s$. Since $\eta \notin \mathbb{F}_s$, the diagonal elements of the triangular form of $\boldsymbol{A}_{\mathcal{I}}$ are all non-zero, implying that $\boldsymbol{A}_{\mathcal{I}}$ is regular. ∎

V. Non-GRS MDS Twisted Codes

Since GRS codes are always MDS and well studied, we will in this section show that most of the twisted codes are not equivalent to an RS code. The main result is the following theorem.

Theorem 18: Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ and $2 < k < n - 2$. Furthermore, let $\mathcal{H} \subseteq \mathbb{F}_q$ satisfy that the twisted code $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ is MDS for all $\eta \in \mathcal{H}$. Then there are at most 6 choices of $\eta \in \mathcal{H}$ such that $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ is equivalent to an RS code.

Proof: Since $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ is an MDS code, it has a generator matrix of the form $\boldsymbol{G} = [\boldsymbol{I} \mid \boldsymbol{A}]$. Equivalently, there exist polynomials $f^{(i)} \in \mathcal{V}_{k,t,h,\eta}$ such that for all i and j in $1, \ldots, k$ it holds that $f^{(i)}(\alpha_j) = 1$ if $i = j$ and $f^{(i)}(\alpha_j) = 0$ if $i \neq j$. Further for $j > k$ we have $f^{(i)}(\alpha_j) = \boldsymbol{A}_{i,j-k}$. In particular, since $f^{(i)} \in \mathcal{V}_{k,t,h,\eta}$, the (i,j)th entry of $\boldsymbol{A}$ is of the form $\boldsymbol{A}_{i,j} = c_{i,j} + d_{i,j}\eta$ for certain $c_{i,j}, d_{i,j} \in \mathbb{F}_q$.

Now we use item (iii) of Theorem 1 to derive an upper bound on the number of choices of η such that $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ is equivalent to an RS code. Let us consider the minor M of the first three rows and columns of $\tilde{\boldsymbol{A}}$. Then $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ is not equivalent to an RS code if M does not vanish. However, since $\tilde{\boldsymbol{A}}_{i,j} = \frac{1}{c_{i,j} + d_{i,j}\eta}$, this minor is of the form

$$M = \frac{p(\eta)}{\prod_{i,j=1}^{3}(c_{i,j} + d_{i,j}\eta)},$$

where $p(\eta)$ is a polynomial in η of degree at most 6. Hence M can vanish for at most six values of η, which implies the theorem. ∎

Theorem 18 directly implies the existence of non-GRS MDS twisted codes for many field sizes, as appears from the following corollaries.

Corollary 19: Suppose $(\mathbb{F}_q^*, \cdot)$ has a non-trivial subgroup G such that $|\mathbb{F}_q^* \setminus G| > 6$. Then for any n, k with $2 < k < n - 2$ and $n \leq |G|$ there exists a non-GRS MDS $(*)$-twisted code. Similarly if $(\mathbb{F}_q, +)$ has a non-trivial subgroup V such that $|\mathbb{F}_q \setminus V| > 6$, then for any n, k with $2 < k < n - 2$ and $n \leq |V|$ there exists a non-GRS MDS $(+)$-twisted code.

Corollary 20: Let $\mathbb{F}_s \subsetneq \mathbb{F}_q$ with $|\mathbb{F}_q \setminus \mathbb{F}_s| > 6$. Let $2 < k < n - 2$ and $n \leq s$. Then, there exists $\eta \in \mathbb{F}_q \setminus \mathbb{F}_s$ such that $\mathcal{C}_k(\boldsymbol{\alpha}, t, h, \eta)$ is MDS but not equivalent to a GRS code.

Remark 21: From $q \geq 13$, non-GRS $(*)$-twisted or $(+)$-twisted codes of length $\lceil (q+1)/2 \rceil$ is guaranteed by Corollary 19. If $q = p^m$ is a prime power with $p > 3$ and $m > 1$, then the restriction $|\mathbb{F}_q \setminus \mathbb{F}_s| > 6$ of Corollary 20 is fulfilled for all $\mathbb{F}_s \subsetneq \mathbb{F}_q$.

VI. Computer Searches

In this section, we present exhaustive computer searches for twisted codes over small field sizes. Since we are most interested in non-GRS codes, we only perform searches for $\eta \neq 0$ and $\min\{k, n-k\} > 2$ (cf. Corollary 2). The compututations were carried out using SageMath v7.4 [10]. The full results and the source code can be downloaded from http://jsrn.dk/code-for-articles.

A. Number of $(*)$-Twisted Codes

We counted all $(*)$-twisted codes over $\mathbb{F}_q$ for $q \leq 19$ and all $(+)$-twisted codes over $\mathbb{F}_q$ for $q = 16$ and $q = 49$, i.e., the number of sets S and η's that fulfill the conditions of Definition 7 respectively Definition 8. Moreover, we have determined how many of the resulting codes are inequivalent and which of those are not GRS codes.

As predicted, for odd q, there are $(*)$-twisted codes of length up to $\frac{q+1}{2}$ and arbitrary k. It also turns out that almost all $(*)$-twisted codes are non-GRS. In particular, there is exactly 1 $(*)$-twisted $[11, 6, 3]$ code which is not GRS, even though Corollary 2 did not guarantee this.

Table I exemplifies the results for $q = 19$.

Table I
Number of $(*)$-twisted codes over $\mathbb{F}_{19}$ (Total / Inequivalent / Non-GRS).

$n \backslash k$	3	4	5	6	7
6	1974/73/67				
7	1092/67/67	1092/63/63			
8	405/25/25	405/25/25	405/25/25		
9	90/7/7	90/6/6	90/6/6	90/7/7	
10	9/2/2	9/1/1	9/1/1	9/2/2	9/1/1

B. Comparison with Roth–Lempel Codes

Roth and Lempel [4] gave a construction of non-GRS MDS codes: given $S \subset \mathbb{F}_q \cup \{\infty\}$ with $n = |S|$ which is *not* a $(k-1)$-sum generator of $(\mathbb{F}_q, +)$, it produces an $[n, k]$ MDS code[2]. Roth and Lempel point out, similar to our Definition 8, that e.g. subgroups of $\mathbb{F}_q$ will give such non-$(k-1)$-generators.

[2]We say that a set S containing ∞ is a k-sum generator if $S \setminus \{\infty\}$ is a k-sum generator. Note that for comparison with our codes, we relax the construction of [4] by allowing S which does not contain ∞.

When q is even, these explicit constructions allow codes in a similar range as $(+)$-twisted codes. When q is odd, their construction is much worse; for q an odd prime, they remark in [9] that asymptotically their construction has at most length $\frac{q}{k}(1+o(1))$.

For small q one can exhaustively search for all non-$(k-1)$-sum generators, however, and thereby produce all Roth–Lempel (RL) codes. We have done this for some parameters with the aim of determining how often $(*)$-twisted or $(+)$-twisted codes are equivalent to RL codes; especially for the $(+)$-twisted codes where the possible range of parameters largely coincides.

Our computer searches indicate that the code families are largely independent. We give three examples:

For $(q,n,k)=(13,7,3)$, there are 35 inequivalent RL codes, while there are 2 $(*)$-twisted codes; 1 code is in both sets. There are no $(+)$-twisted codes of these parameters, but there are 8 twisted codes with $(t,h)=(1,k-1)$; 2 of these are RL codes.

For $(q,n,k)=(16,8,5)$, there are 186 inequivalent RL codes, while there are 9 inequivalent $(+)$-twisted codes. These codes are all different. There are 83 twisted codes in total with $(t,h)=(1,k-1)$, and 10 of these are RL codes.

For $(q,n,k)=(23,12,5)$, there are no RL codes, while there is 1 equivalence class of $(*)$-twisted codes.

C. Length $\approx q/2$ Codes with "Exotic Twists"

$(*)$-twisted and $(+)$-twisted codes are explicit subclasses of the cases $(t,h)=(1,0)$ respectively $(t,h)=(1,k-1)$ which allow codes of length $\approx q/2$ for odd respectively even q. A natural question is if similar long MDS codes are possible for twisted codes of other (t,h).

We have no explicit construction, but exhaustive search indicates a resounding 'yes': in fact, for any $q \leq 19$ we verified that for almost *any* choice of (t,h) there is an $[n,k]$ twisted MDS code for $n=\lfloor q/2 \rfloor$ and $3 \leq k \leq n-3$, with the only exceptions being $(t,h)=(1,k-1)$ which fails for $(q,k)=(17,4)$ and $q=19$ and any k.

The non-existence for $(t,h)=(1,k-1)$ should indeed be expected for high enough k due to Lemma 13 and the asymptotic upper bounds on $M(k,\mathbb{F}_q)$ discussed in [9]. However, it is surprising and intriguing that for all other (t,h), there seem to be long twisted MDS codes.

D. Counting Twisted MDS Codes

Table II enumerates all MDS twisted codes for $q \leq 13$, the number of equivalence classes as well as non-GRS equivalence classes. We see that many parameters often lead to equivalent codes: e.g. for $(q,n,k)=(13,7,4)$, each equivalence class is obtainable by $\approx$1200 parameters on average. This might be due to algebraic symmetries in the parameter choices, which is an interesting question to investigate. However, most MDS twisted codes are non-GRS. Note that in most of the cases, we can construct codes of length $q-1$ for $k \in \{3, n-3\}$. Apart from Glynn's code and its dual [11], we find only a single new code of length q: $(q,n,k)=(8,8,5)$ and constructible as e.g. $\mathcal{C}_5(\boldsymbol{\alpha},1,4,1)$ with $\boldsymbol{\alpha}=\mathbb{F}_8 \cup \{\infty\} \setminus \{1\}$. This code is also equivalent to a Roth–Lempel code.

VII. Decoding of Twisted Codes

A simple decoding paradigm is possible for twisted codes: guess the value of the hook coefficient a_h, and then apply an $[n,k]$-RS decoding algorithm on $r-\mathrm{ev}_{\boldsymbol{\alpha}}(\eta a_h x^{k-1+t})$, where r is the received word. If the twisted code is over $\mathbb{F}_q$, this will apply the RS decoder q times. This works with errors, erasures, soft-decision, list-decoding, etc. In particular, we have (cf. [12]):

Theorem 22: An $[n,k]$ twisted code over $\mathbb{F}_q$ can be decoded up to half the minimum distance in complexity $O\tilde{}(qn)$.

Note that even if the twisted code is not MDS, this approach still gives a list-decoder up to $(n-k+1)/2$: collect the codewords obtained from each guess of a_h, and the correct codeword is on the resulting list if the number of errors is at most the decoding radius of the RS decoder.

VIII. Conclusion

We have introduced twisted Reed–Solomon codes, a new class of $\mathbb{F}_q$-linear codes, and demonstrated that for $q \geq 7$ the class contains many new non-GRS MDS codes. We singled out two explicit subclasses, $(*)$-twisted and $(+)$-twisted codes, with which we can construct MDS codes of length at least $q/2$ for any field size q, and that for most field sizes, most of these codes will be non-GRS. Using computer searches we demonstrated that there seems to be many other and longer MDS, non-GRS twisted RS codes.

References

[1] R. Singleton, "Maximum Distance q-nary Codes," *IEEE Trans. Inf. Theory*, vol. 10, no. 2, pp. 116–118, 1964.

[2] I. S. Reed and G. Solomon, "Polynomial Codes over Certain Finite Fields," *SIAM*, vol. 8, no. 2, pp. 300–304, 1960.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Elsevier, 1977.

[4] R. M. Roth and A. Lempel, "A construction of non-Reed-Solomon type MDS codes," *IEEE Trans. Inf. Theory*, vol. 35, no. 3, pp. 655–657, May 1989.

[5] R. M. Roth and G. Seroussi, "On Generator Matrices of MDS Codes (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 31, no. 6, pp. 826–830, 1985.

[6] J. Sheekey, "A New Family of Linear Maximum Rank Distance Codes," *Advances in Mathematics of Communications*, vol. 10, pp. 475–488, 2016.

[7] R. Roth, *Introduction to Coding Theory*. CUP, 2006.

[8] R. M. Roth and A. Lempel, "On MDS Codes via Cauchy Matrices," *IEEE Trans. Inf. Theory*, vol. 35, no. 6, pp. 1314–1319, 1989.

[9] ——, "t-sum generators of finite Abelian groups," *Discrete Mathematics*, vol. 103, no. 3, pp. 279–292, May 1992.

[10] W. A. Stein *et al.*, "SageMath Software," http://www.sagemath.org.

[11] D. G. Glynn, "The non-classical 10-arc of PG (4, 9)," *Discrete mathematics*, vol. 59, no. 1, pp. 43–51, 1986.

[12] J. Justesen, "On the complexity of decoding Reed-Solomon codes (Corresp.)," *IEEE Transactions on Information Theory*, vol. 22, no. 2, pp. 237–238, Mar. 1976.

Table II
Counting MDS Twisted Codes
(Total/Inequivalent/Non-GRS. Blank = 0/0/0)

q	n	$k=3$	4	5	6	7	8	9
7	6	38/3/2						
8	6	406/5/4						
	7		63/2/1					
	8			14/2/1				
9	6	2374/7/5						
	7	216/3/3	332/3/2					
	8	4/1/1	40/1/1	36/1/1				
	9		4/1/1	4/1/1				
11	6	32518/15/11						
	7	6286/21/19	8554/20/18					
	8	585/15/15	160/7/6	960/9/7				
	9	40/3/3		20/1/0	135/1/0			
	10	2/1/1				22/2/1		
13	6	216722/26/21						
	7	71618/80/75	98430/80/75					
	8	11164/165/160	5176/98/93	26916/139/134				
	9	1110/32/31	41/4/3	381/8/5	5424/24/21			
	10	138/4/4			93/3/0	1167/4/1		
	11	24/1/1					254/1/0	
	12	2/1/1						26/2/1